VERMONT
AGENCY OF HUMAN SERVICES

State of Vermont
Agency of Human Services (AHS)

Policy Title: Information Security Assessment and Authorization Policy	**Policy No. 5.08 v.2** **Revision History Date:** Current Version - 10/23/18
Attachments/Related Documents:	**Revision Number:**
Name/Title of Authorizing Signature: Martha Maksym, Acting Secretary	**Effective Date: 10/24/19**
☒**Trauma Informed Review**	

Authorizing Signature:

POLICY STATEMENT:

To establish high-level requirements, organizational responsibilities, and managerial commitment for an Information Security Assessment and Authorization Policy that ensures the confidentiality, integrity, and availability of information and systems within the Agency of Human Services (AHS) in compliance with all applicable State and Federal Laws, regulations, or policies.

BACKGROUND:

The HIPAA Security Rule (45 CFR § 164.308(a)(8)) requires AHS to perform periodic technical and nontechnical evaluations, in response to environmental or operational changes affecting the security of electronic protected health information (ePHI), that establishes the extent to which an entity's security policies and procedures meet the requirements of the HIPAA Security Rule administrative safeguards. The HIPAA Security rule (45 CFR § 164.308(a)(2)) requires AHS to designate a security official who is responsible for implementing its security policies and procedures. The HIPAA Security Rule (45 CFR § 164.308(a)(1)(ii)(D)) also requires AHS to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

AHS uses Security Assessments to review the risks and security controls in designated information systems to determine the extent to which controls are implemented correctly, operating as intended, and producing the desired outcomes for meeting security requirements.

AHS Security Authorizations are official management decisions which authorize the operation of information systems and to explicitly accept the risk to organizations and assets, individuals, and other organizations based on the implementation of agreed-upon security controls.

DEFINITIONS:

Security Controls - The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information (as defined in National Institute of Standards and Technology (NIST) 800-53, Appendix B).
POA&M - a Plan Of Action and Milestones that documents the organization's planned, implemented, and evaluated remedial actions to correct deficiencies noted during assessments of the security controls to reduce or eliminate known vulnerabilities in the system.

SCOPE:

This policy governs: 1) AHS information security assessments and security controls in designated information systems; and 2) official management security authorizations for the operation of information systems.

ROLES AND RESPONSIBILITIES:

AHS Secretary – Responsible for making a final review and approval of this policy.
AHS Policy Committee - Responsible for making a final review of this policy.
Chief Information Security Officer (CISO) – Responsible for:

- reviewing and approving this policy prior to AHS Policy Committee; and
- ensuring all necessary information systems are properly integrated into security assessment and authorization activities.

Authorizing Official - Responsible for:

- authorizing the operation of information technology systems in accordance with this policy.

AHS Information Security Director – Responsible for:

- scheduling and coordinating security assessments of existing information technology systems at least annually and reports results to the CISO and the Authorizing Official.
- scheduling and coordinating security assessments of all new information technology systems prior to deployment and reports results to the CISO and the Authorizing Official.
- creating procedures and standards to meet the requirements established in this policy;
- reporting all matters pertaining to the AHS's compliance with this policy to the CISO and the Authorizing Official;
- establishing criteria for designating information technology systems to be assessed; and
- ensuring that this policy is reviewed and updated (if necessary) at least annually.

PROTOCOLS:

Plan of Action and Milestones (POA&M)

AHS will maintain POA&M documents that outline the known issues identified in information systems during internal and third-party security assessments, and informal discovery processes. AHS will update POA&Ms on a regular basis and as progress is made on identified issues, and new items are added as they are discovered. The AHS Information Security Director will submit POA&Ms to appropriate Federal entities as required. Automated mechanisms will be employed to help ensure that POA&Ms for the information systems are accurate, up to date, and readily available.

Security Assessment and Continuous Monitoring

A combination of internal and independent assessors will be used to conduct assessments of the security controls of the information systems on annual basis. Automated or manual assessments are to be planned, scheduled and conducted on a continuous or unannounced basis of all information systems. Penetration testing will be announced to ensure compliance with all vulnerability mitigation procedures as well as in-depth monitoring of systems and networks. The AHS Information Security Director will monitor the security controls in the information systems on an ongoing basis in accordance with the continuous monitoring standards.

Security Authorization

- AHS Information Security Director notifies Authorizing Officials of security risks prior to implementation of a new system.
- Security authorizations are official management decisions by AHS Appointing Authorities, or their designees (Authorizing Official) conveyed through authorization decision documents, to authorize the operation of information systems. Such documentation will explicitly accept the risk to organizational operations and assets, individuals, and other organizations based on the implementation of agreed-upon security controls. Authorizing officials provide budgetary oversight for organizational information systems or assume responsibility for the mission/business operations supported by those systems. Through the security authorization process, authorizing officials assume responsibility and are accountable for security risks associated with the operation and use of organizational information systems. Accordingly, Authorizing Officials are in positions with levels of authority commensurate with understanding and accepting such information security-related risks. Authorizing Officials:
    - accept the risks to organizational operations and assets, individuals, and other organizations based on the implementation of agreed-upon security controls,
    - provide budgetary oversight for organizational information systems or assume the responsibility for the mission/business operations supported by those systems, and
    - accept security risks associated with the operation and use of organizational information systems.

The security authorization for each information system will be documented by the Authorizing Official for their information system(s) prior to operation and updated at least every three years or more frequently to include the cases listed below:

- When there are substantial changes to the system or changes in the requirements that result in

the need to process data of a higher sensitivity.
- When changes occur to authorizing legislation or federal requirements.
- After the occurrence of a serious security violation.
- Prior to expiration of a previous security authorization.

Information System Connections

Connections from the information system to other information systems outside the authorization boundary shall be authorized in accordance with the use of Interconnection Security Agreements (ISA). The ISA includes details for each connection, interface characteristics, security requirements, and the nature of the information communicated. The information system connections will be monitored and renewed on an ongoing basis in order to verify enforcement of security requirements. The information system will have a deny all, allow by exception process in place when connecting internal information systems that receive, process, store or transmit personally identifiable information (PII), personal health information (PHI) and Federal tax information (FTI), to external information systems.

ENFORCEMENT:

The AHS Secretary may initiate reviews, assessments or other means to ensure that policies, guidelines or standards are being followed.

AUTHORITIES:

- Health Insurance Portability and Accountability Act (HIPAA) Security Rule: 45 CFR Part 160 and Subparts A and C of Part 164;
- Centers for Medicare and Medicaid Services (CMS), Minimum Acceptable Risk Standards for Exchanges (MARS-E)
- IRS Publication 1075
- Social Security Administration (SSA), *Electronic Information Exchange Security Requirements and Procedures For State and Local Agencies Exchanging Electronic Information With The Social Security Administration* based on: Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347, the Privacy Act of 1974 and SSA's own policies, procedures and directives
- Criminal Justice Information Services (CJIS), Security Policy
- National Institute of Standards and Technology (NIST) Special Publication 800-53, Information Security
- NIST Special Publication 800-30, Risk Management, (NIST Special Publications available at http://csrc.nist.gov/publications/PubsSPs.html)
- AHS Policy 1.01: Policy on Policies

REFERENCES:

MARS-E	IRS Pub 1075	SSA	HIPAA	CJIS
CA-1 CA-2 CA-2 (1) CA-3 CA-3 (5)	9.3.4.3	5.6 6.2	§164.308(a)(1)(ii)(D) §164.308(a)(2) §164.308(a)(8)	

CA-5 CA-6 CA-7 CA-7 (1)				

Document Review and Revision Control			
Version	**Review Date**	**Author/Reviewer**	**Description**
1.0	10/18/19	Emily Wivell	Revised Policy 5.08 Effective 10/23/08; repeal VHC-POL-CA effective 3/21/19 and DCF POL-CA effective 11/1/17.

APPENDIX:

None.